



PKI/Medium Grade Services Interoperability Summit *'Tech Fest 2000'*

Betsy Appleby
APPLEBYB@NCR.DISA.MIL
(703) 681-0283
24 March 00



Why Are We Here

- **To address interoperability issues with PKI and COTS email products**
- **To share solutions**
- **To define test scenarios**
- **To establish a process for documenting problems/solutions**
- **To promote vendor involvement**
- **To move ahead with DOD MGS roll-out**

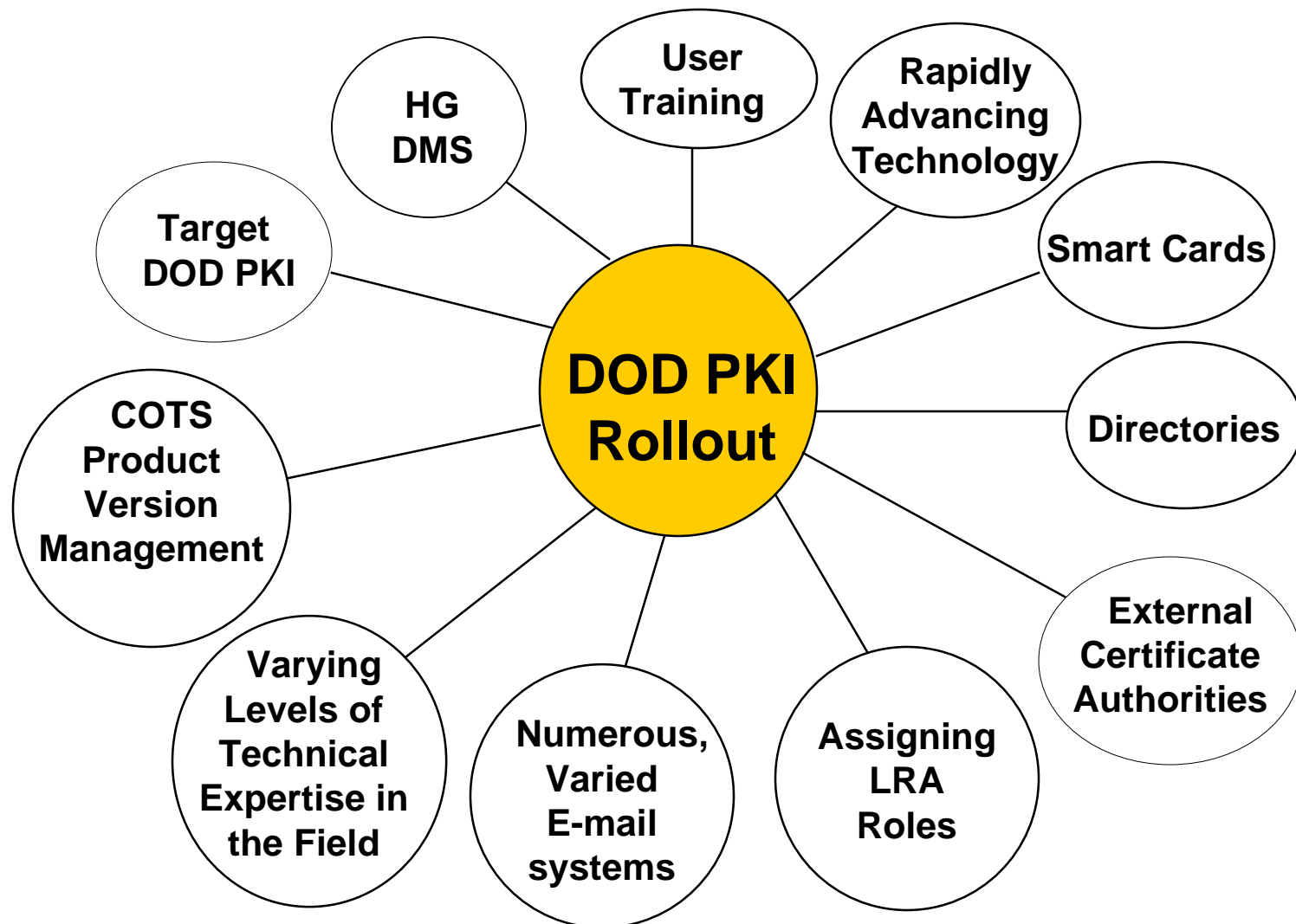


What is DMS/MGS?

**DMS/MGS is secure interoperable
commercial off-the-shelf (COTS) email
that uses
the DOD Public Key Infrastructure (PKI)
Medium Assurance certificates
for signature and encryption**



MGS/PKI Problem Space

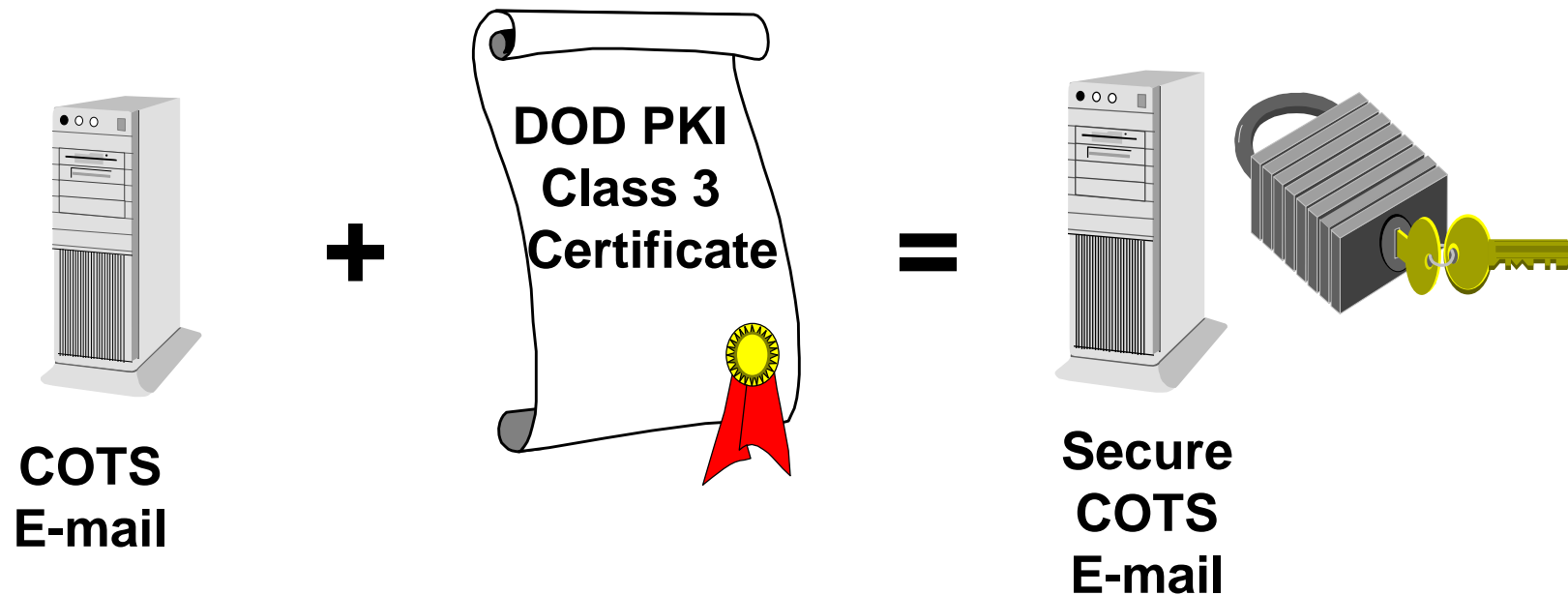




DMS/MGS

PKI and MGS

In MGS, the DoD PKI provides an e-mail certificate that is bound to the user's e-mail address and enables the user to send and receive signed and encrypted e-mail to and from other MGS users.





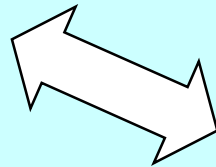
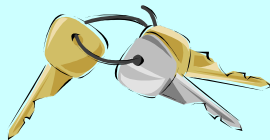
MGS Ground Rules

- **MGS = COTS**
- **MGS will use DOD PKI Medium Assurance Certificates for Signature and Encryption**
- **Trust BUT Verify testing approach**
 - **Multi-vendor product interoperability**
 - **DOD PKI readiness**
- **Gain early operational experience through pilots**



MGS Activities

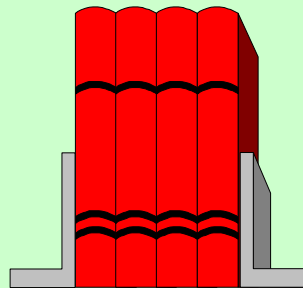
DoD PKI



Netscape
Communicator 4.7



1. Lab Integration



2. Create User Documentation

5th Signal



3. Pilot Rollout



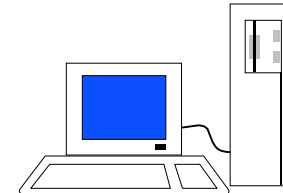
Lab Activities Completed

1. Installed and Configured

- Clients (on Windows 95, 98, NT)
 - MS Outlook '98
 - MS Outlook Express 5
 - Netscape Communicator 4.7
 - Lotus Notes 5.01a

- Servers:

- MS Exchange 5.5 SP2
- Lotus Notes 5.01a



2. Executed Comprehensive Interoperability Test Suite

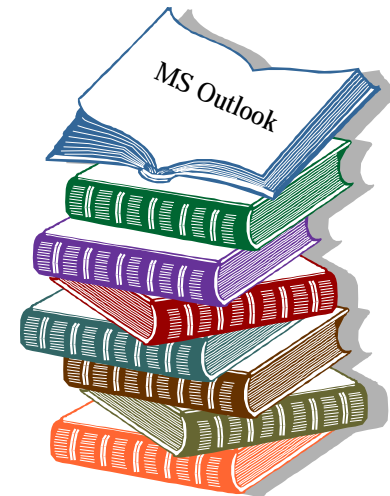
- Signed
- Encrypted
- Signed and Encrypted



MGS Products

Verified for Interoperability

- **Generated Step-By-Step User's Guides for the Retrieval of DOD PKI Certificates and Configuration of E-mail Clients**
 - Lotus Notes 5.01a
 - Microsoft Outlook Express 5.0
 - Microsoft Outlook 98/2000
 - Netscape Communicator 4.7





Background Policy

Driving the MGS High Demand

Deputy Secretary of Defense Memorandum, 6 May 1999, Department of Defense (DoD) Public Key Infrastructure (PKI)

- **All DoD Users will, at a minimum, be issued a Class 3 certificate by October 2001**
- **All electronic mail (as distinct from organizational messaging) sent within the Department will be signed using appropriate protocols consistent with the Department's email strategy by October 2001**
- **Department of Defense components are encouraged to encrypt email within the Department**



MGS Pilot Criteria

- **Each pilot brings unique scenarios**
 - **USAREUR - Replace PGP - 'Train the Trainer' - Roving kiosks for registration**
 - **USMC - IECAs - USMC Email Policy**
 - **USAF - Registration using 'trusted agents'**
- **Pilot partner must document and disseminate lessons learned**
- **MGS Pilot solutions MUST be scalable**



Definition: IECA

- **Interim External Certification Authorities (IECAs)**
 - Certification Authorities that provided non-DOD personnel with certificate services that are interoperable with the DOD PKI
 - Operated by organizations other than the DOD
 - IECA certificates not signed by the DOD Root; hence DOD applications use IECAs as trust anchors
 - Short-Term Solution for DOD

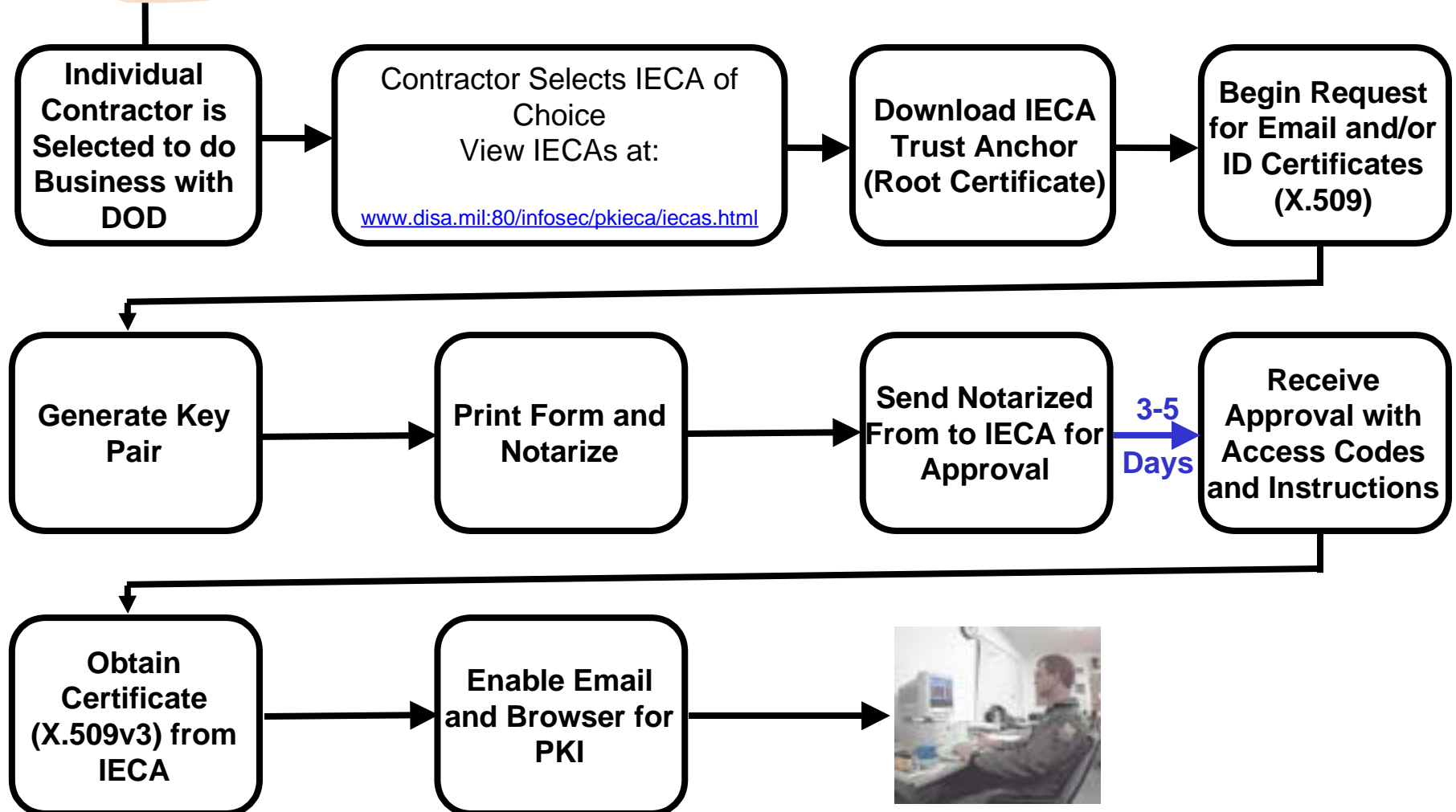


IECA Vendors

- **Operational Research Consultants (ORC)**
- **Digital Signature Trust (DST)**
- **VeriSign, Inc.**
- **General Dynamics**



DOD Trading Partner PKI User Registration Process





IECA REGISTRATION COMPARISON

	DST https://secure.digsign.com/ieca/	GD http://gd.cs.com/ieca	ORC http://eca.orc.com/index2.html	VeriSign http://www.verisign.com/gov/ieca/
Supported Browsers (FIPS 140-1)	Netscape 4.05 > (Domestic)		Netscape 4.05> (Domestic)	Netscape 4.05 > IE 5.01 > (Domestic)
Certificate Pricing / year	ID - \$250 Email - \$250		ID - \$ N/A Email - \$ N/A	ID - \$195 Email - \$195
Identity Validation	Both - \$475 Face-to-Face or Notary (applying organization or Financial institution only) with: - 1 Government Photo ID		Both - \$250 Face-to-Face or Notary (any) with: - Drivers License	Both - \$295 Face-to-Face or Notary (any) with: -1 Government Photo ID -2 Other ID
Key Generation	At time of Registration		At time of Registration	Upon Approval via email
Approval Notification	U.S. Mail		Email	Email
Turn Around Time	13 days (Notary Denied, I didn't follow directions and approval via U.S mail)		5 days	4 days



How to *Operationalize* MGS

- **Establish Technical Environment**
 - RA/LRA Technical Infrastructure(people/HW/SW)
 - Email product & Internet browsers meet minimal requirements
 - Support staff and core users are postured for MGS
- **Define Process/Publish Procedures**
 - Outline the process of registering and enabling email
 - Provide step-by-step procedures
 - Identify MGS cadre to capture lessons learned



How to *Operationalize* MGS (cont.)

- ***Train the Trainers*** with classroom & hands-on instruction
 - Register and train support staff and power users
 - Train Help Desk
 - Train initial core group in using MGS in daily activities
- **Follow-up - *Building on Success***
 - Provide third-tier support
 - Collaborate with COTS email vendors to solve systematic problems
 - Provide Updates/Enhancements to MGS User Base



COTS Facts of Life

- **New product releases and versions occur frequently**
- **COTS versions generally newer than fielded DMS User Agents**
- **Configuration is Everything!**
 - **A wide variety of configurations will work for basic SMTP**
 - **Only a few configurations will work for MGS**
 - **Pilot sites often have heterogeneous configurations installed**



MGS Bottom Line

- **MGS is PKI Ready and being used today**
 - *PKI Ready is Changing*
- **Email crosses all boundaries and is on every desktop**
- **The time is right for MGS implementation**
- **Continue work with vendors, develop tools, test products & processes, and manage knowledge for the benefit of all DOD users**

MGS is not a *product* - it is a *capability*



MGS/PKI Interoperability Summit GOALS

- **Resolve 'Top 5' Issues**
- **Build the DOD secure COTS email 'interest group'**
- **Identify top priority interoperability test scenarios**
- **Work together to continue technical dialog beyond this summit**



Back-Up Charts
